P03358810E1-7

METHOD FOR CONTROLLING ACCESS

Patent Number: ☐ WO0223801

Publication date: 2002-03-21

Inventor(s): VOLLMER VASCO (DE); HOFMANN MATTHIAS (DE)

Applicant(s): BOSCH GMBH ROBERT (DE); VOLLMER VASCO (DE); HOFMANN MATTHIAS (DE)

Requested Patent: ☐ DE10045975

Application Number: WO2001DE03474 20010911

Priority Number(s): DE20001045975 20000916

IPC Classification: H04L12/00

EC Classification:

Equivalents:

Abstract

According to the invention, access to elements within a bus system or network may be controlled whereby an external device (100) identifies itself by means of a device-specific code with a bus or network manager (300). After authentication by means of a digital key the external device is given access according to the specific class thereof to elements of the bus system or network.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 45 975 A 1**

(51) Int. Cl.[7]: **H 04 L 9/32**

(21) Aktenzeichen: 100 45 975.7
(22) Anmeldetag: 16. 9. 2000
(43) Offenlegungstag: 11. 4. 2002

DE 100 45 975 A 1

(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

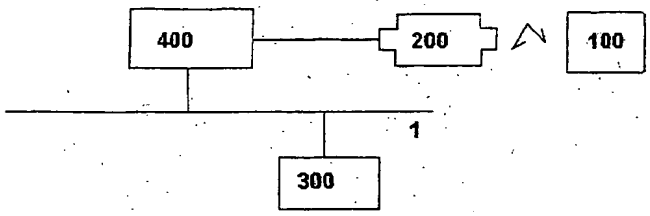
(72) Erfinder:
Vollmer, Vasco, 29471 Gartow, DE; Hofmann, Matthias, 31141 Hildesheim, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Steuerung des Zugriffs

(57) Zur Steuerung des Zugriffs auf Elemente innerhalb eines Bussystems oder Netzes identifiziert sich ein externes Gerät (100) über eine gerätespezifische Kennung bei einem Bus- oder Netzmanager (300). Nach einer Authentifizierung anhand eines digitalen Schlüssels wird dem externen Gerät ein Zugriff entsprechend seiner Zugehörigkeit zu einer bestimmten Klasse auf Elemente des Bussystems oder Netzes gewährt.



DE 100 45 975 A 1

Beschreibung

Stand der Technik

[0001] Die Erfindung geht aus von einem Verfahren zur Steuerung des Zugriffs auf Elemente innerhalb eines Bussystems oder Netzes.

[0002] Aus dem IEEE Standard **1394** [1] ist ein serielles Bussystem bekannt, bei dem verschiedene Endgeräte (Knoten) entweder über ein 4–6-adriges Kabel oder einen Lichtwellenleiter angeschlossen werden. Mindestens ein Knoten kann dabei in der Art ausgeführt sein, dass er zusätzliche Verwaltungsfunktionen für das Netzwerk übernehmen kann (Busmanagement).

[0003] Neben obigem Standard gibt es eine busunabhängige Erweiterung, die unter dem Namen HAVi (Home Audio Video interoperability) [2] spezifiziert ist. Diese HAVi-Spezifikation beschreibt insbesondere die Fern-Kontrolle von Geräten unter Verwendung eines Ressourcen-Managers, der eine Ressource (Gerät) auf Anforderung belegt und sie auch wieder freigibt.

[0004] In der HAVi-Spezifikation wir ein verteiltes Modell beschrieben, bei dem die Steuerung der Geräte über Kontrollmodule, sogenannte "Device Control Modules (DCM)", vorgenommen wird. Diese DCM laufen als Softwareelement auf dem Gerät, das Kontrollfunktionen auf einem anderen Gerät ausführen will. Dabei ist ein DCM jeweils spezifisch für ein bestimmtes Gerät oder eine Geräteklasse.

[0005] Der HAVi-Standard bietet die Möglichkeit, einem Softwareelement zwei verschiedene Sicherheitsstufen zuzuweisen. Dabei wird ein Softwareelement als "trusted" bezeichnet, wenn dieses vom Hersteller ausreichend getestet wurde. Bei Softwareelementen, die dynamisch in das System geladen werden, muss über eine digitale Signatur die Authentizität des Softwareelements nachgewiesen werden. Alle DCMs müssen den Status "trusted" haben. Als "untrusted" werden diejenigen Softwareelemente bezeichnet, die vom Hersteller nicht als "trusted" markiert wurden. Auf Basis dieser Einstufung entscheidet der Empfänger einer Anforderung, ob er dem sendenden Softwareelement vertraut, das heißt auch ein "untrusted" Softwareelement kann Anforderungen senden, es ist jedoch nicht sicher, ob diese Anforderung erfüllt wird.

Vorteile der Erfindung

[0006] Mit den Maßnahmen des Anspruchs 1 ist eine Sicherheitsfunktion gewährleistet, die insbesondere für den Einsatz in heterogenen Netzen, z. B. im Kraftfahrzeug, eine weitergehende Sicherheit gewährleistet als sie mit dem HAVi-Standard zu erreichen ist. Insbesondere eignet sich die Erfindung bei der Kommunikation zwischen und mit Softwareelementen über verschiedene Bus- und/oder Netzwerktechnologien. Es wird eine eindeutige Identifikation von Geräten, beziehungsweise Softwareelementen innerhalb eines Netzes erreicht, das beispielsweise nach dem HAVi-Standard arbeitet. Ein Gerät oder Softwareelement wird anhand einer gerätespezifischen Kennung als Gerät einer bestimmten Klasse erkannt. Die Authentizität eines Gerätes beziehungsweise Softwareelementes wird anhand eines digitalen Schlüssels festgestellt. Nach der Authentifizierung wird dem Gerät ein Zugriff entsprechend seiner Klassenzugehörigkeit auf Elemente des Bussystems oder Netzes gewährt.

[0007] In den Unteransprüchen sind vorteilhafte Ausgestaltungen aufgezeigt.

[0008] Gemäss Anspruch 2 ist es von Vorteil, dass sich ein externes Gerät für den Zugriff bei einem Gateway mittels einer Anmeldenachricht anmeldet, welche insbesondere zusammen mit der Gerätekennung zum Bus- oder Netzmanager übertragen wird.

[0009] Nach Anspruch 3 wird neben der gerätespezifischen Kennung auch eine Geräteklassenkennung übertragen, anhand derer der Zugriff gesteuert werden kann.

[0010] Durch die gemeinsame Schlüsselvereinbarung gemäss den Ansprüchen 4 und 5 insbesondere unter Verwendung des Diffie-Hellman Key-Exchange kann ein Dritter diesen Schlüssel nicht ermitteln.

[0011] Nach Anspruch 6 wird nach der gemeinsamen Schlüsselvereinbarung eine Authentisierung nach dem Challenge-Response-Verfahren durchgeführt.

[0012] Durch die Maßnahmen des Anspruchs 7 können sowohl Signalumsetzungen nach dem ISO/OSI-Schichtenmodell in der Physical-Layer wie auch in höheren Schichten, z. B. Adressumsetzungen, durchgeführt werden.

[0013] Das Gateway kann nach Anspruch 8 vorteilhaft mit einer Firewallfunktionalität ausgestattet werden, um einen unberechtigten Zugriff von einem anderen Netz zu verhindern.

[0014] Gemäss Anspruch 9 kann die Authentisierung dazu benutzt werden, festzustellen, welche Ressourcen des Bussystems oder Netzes ein externes Gerät auf welche Art und Weise und/oder kontrollieren darf.

[0015] Der Bus- oder Netzmanager kann nach Anspruch 10 vorteilhaft die aufgrund der von ihm ermittelten Zugriffsberechtigung die Firewallfunktionalität so konfigurieren, dass diese die Freigabe oder Sperrung der Ressourcen im Bussystem oder Netz vornimmt.

[0016] Die Freigabe oder Sperrung kann gemäss Anspruch 11 vorteilhaft aufgrund der Quell- oder Zieladresse eines Datenpaketes vorgenommen werden.

[0017] Nach Anspruch 12 kann die Firewallfunktionalität entsprechend der ermittelten Zugriffsberechtigung, bestimmte Kommandos eines externen Gerätes filtern.

[0018] Anstelle einer festen Zuweisen der Zugriffsberechtigung durch den Bus- oder Netzmanager, kann gemäss Anspruch 13 die Zugriffsberechtigung ausgehandelt werden.

[0019] Anstelle eines externen Gerätes, kann gemäss Anspruch 14 auch ein ganzes externes Bussystem oder Netz eine Kommunikationsverbindung aufnehmen, um einen Zugriff auf Elemente des Bussystems oder Netzes zu erhalten.

Zeichnungen

[0020] Anhand der Zeichnungen werden Ausführungsbeispiele der Erfindung erläutert. Es zeigen

[0021] **Fig.** 1 die Netztopologie eines Bussystems,

[0022] **Fig.** 2 verschiedene Netzelemente,

[0023] **Fig.** 3 die Authentisierung am Busmanager.

Beschreibung von Ausführungsbeispielen

[0024] Die Erfindung wird anhand des seriellen Bussystems gemäss dem IEEE Standard **1394** [1] erläutert, wobei auch auf die Erweiterung gemäss HAVi-Spezifikation [2] Bezug genommen wird. Vor der eigentlichen Erläuterung der Erfindung wird zum besseren Verständnis auf den IEEE Standard **1394** und die HAVi-Spezifikation eingegangen. Außerdem werden einige Begriffe zum Verständnis erläutert.

[0025] Die verschiedenen Endgeräte (Knoten) sind nach **Fig.** 1 entweder über ein 4–6-adriges Kabel oder einen Lichtwellenleiter **1** angeschlossen. Dabei kann ein Knoten wahlweise als Endstück (Blatt) **200** oder als Relaisknoten (Zweig) **300**, **400** ausgeführt sein. Der oberste Knoten wird

als Wurzel bezeichnet. Durch den Einsatz der verschiedenen Knotentypen kann eine geeignete Topologie des Netzes aufgebaut werden. Ein Blatt empfängt dabei Informationspakete und verarbeitet sie, falls die Ziel-Adresse des Paketes mit der eigenen übereinstimmt. Ein Zweig muss zusätzlich alle Pakete, die er auf einem Port empfängt auf allen anderen Ports aussenden.

[0026] IEEE **1394** sieht vor, dass das Netzwerk selbstkonfigurierend ist, d. h. nach dem Einschalten oder nach einem Reset senden alle Knoten einige ausgewählte Informationen über sich selbst ins Netz. Diese Information wird dabei von allen Knoten empfangen. Ein Knoten kann dabei in der Art ausgeführt sein, dass er zusätzliche Verwaltungsfunktionen für das Netzwerk übernehmen kann (Busmanagement). Dazu sammelt er alle Informationen der anderen Knoten, verarbeitet sie und speichert sie intern geeignet ab. Sollten mehrere Knoten Busmanagementfähigkeiten besitzen, gibt es ein Konkurrenzverfahren, aus dem ein Knoten als Sieger hervorgeht, der dann das Busmanagement übernimmt.

[0027] Neben den Verfahren, wie sie in den Spezifikationen zu IEEE **1394** beschrieben sind, gibt es die busunabhängige Erweiterung HAVi, die für den Einsatz in einem IEEE 1394-Netzwerk geeignet ist. Insbesondere die Fern-Kontrolle von Geräten von jedem anderen Punkt im Netzwerk wird in der HAVi-Spezifikation beschrieben. Dazu ist ein verteiltes Modell beschrieben, bei dem die Steuerung der Geräte über Kontrollmodule, sogenannte "Device Control Modules (DCM)", vorgenommen wird. Diese DCM laufen als Softwareelement auf dem Gerät, das Kontrollfunktionen auf einem anderen Gerät ausführen will. Dabei ist ein DCM jeweils spezifisch für ein bestimmtes Gerät oder eine Geräteklasse. Eine weitere Gruppe von Softwareelementen stellen die "Functional Component Modules" dar, von denen jeweils mehrere hierarchisch unterhalb eines DCM angeordnet werden können und die für die Kontrolle jeweils eines spezifischen funktionalen Teils eines Gerätes zuständig sind.

[0028] Ein Gateway dient der Verbindung zweier Netzwerke untereinander. Dabei wird unterschieden, auf welchem Netzwerklayer (vgl. ISO/OSI-Schichtenmodell) diese Verbindung vorgenommen wird. So ist ein Gateway, welches nur den ersten (physical-Layer) umfaßt, im Wesentlichen nur ein Umsetzer von physikalischen Gegebenheiten, z. B. ein elektro-optischer Wandler, hier werden die eigentlichen Daten nicht verändert. Ein Gateway, das auch höhere Schichten beinhaltet, wertet zusätzlich bestimmte Datenfelder aus und verändert diese gegebenenfalls entsprechend den Erfordernissen des Zielsystems, z. B. kann eine Adressumsetzung der Ziel- und Quelladresse vorgenommen werden, wenn die beiden verbundenen Netze unterschiedliche Adressierungsschemata verwenden.

[0029] Eine Firewall dient der Absicherung eines Netzes gegen einen unberechtigten Zugriff von einem anderen Netz aus, z. B. von einem Teilnetz aus auf ein anderes Teilnetz.

[0030] Bei einer Authentisierung führt ein Kommunikationsteilnehmer einem anderen Kommunikationsteilnehmer gegenüber den Nachweis seiner Identität.

[0031] Der Globally Unique Identifier (GUID) ist eine im IEEE 1394-Standard festgelegte Nummer, die aus einer 24 Bit langen Herstellerkennung und einer 40 Bit langen, vom Hersteller wählbaren Zahl besteht. Die Herstellerkennung wird dabei von der IEEE auf Anfrage eindeutig zugewiesen. Die GUID wird fest in ein IEEE-1394 konformes Gerät gespeichert und identifiziert dieses eindeutig.

[0032] Die Model ID ist ein 24 Bit langes Datenfeld, mit dem der Hersteller eines Gerätes die Zugehörigkeit zu einer bestimmten Geräteklasse oder -Familie kennzeichnen kann.

[0033] Das erfindungsgemäße Verfahren dient dazu, die Authentisierung eines Gerätes durchzuführen, das beispielsweise an ein Fahrzeugnetzwerk angeschlossen wird. Dabei wird im Allgemeinen ein internes Netz mit einem über ein Gateway bereitgestellten externen Anschluß vorgesehen. Dieser Anschluß wird in der Folge als Anwender-Port bezeichnet. Das Gateway ist notwendig, um einerseits die physikalische Umsetzung vorzunehmen, d. h. beispielsweise eine Umsetzung von einem internen Lichtwellenleiter auf einen externen elektrischen oder drahtlosen Anschluß und andererseits gegebenenfalls eine Protokollumsetzung durchzuführen. Außerdem ist unter Umständen die Integration einer Firewall gewünscht, um die Sicherheit des internen Netzes zu gewährleisten.

[0034] Da an den Anwender-Anschluß auch Geräte angeschlossen werden können, die sensitive Daten mit dem internen Netz austauschen, z. B. ein Werkstattdiagnosegerät, ist es notwendig, eine sichere Authentisierung einerseits des angeschlossenen Gerätes, aber auch des Netzes durchzuführen. Das erfindungsgemäße Verfahren verwendet dabei einen Mechanismus zum sicheren Austausch eines Schlüssels, der als Diffie-Hellmann Key-Exchange bekannt ist (siehe [3], Kapitel 7.1.5.2). Außerdem wird eine Authentisierungsprozedur verwendet, die als Challenge-Response Verfahren bekannt ist ([3], Kapitel 7.1.5.1).

[0035] Angenommen werden drei beteiligte Instanzen (**Fig.** 2). Das externe Gerät **100** wird an den Anwender-Anschluß angeschlossen. Dieser ist wiederum über das Gateway **200** an das interne Netzwerk **1** des Fahrzeugs angeschlossen. In diesem Netzwerk dient der Busmaster, beziehungsweise Busmanager oder Netzmanager **300** als eine zentrale Kontrollinstanz, die insbesondere auch die Authentizität angeschlossener Geräte überwacht.

[0036] Nach dem Anschließen des externen Gerätes **100**, meldet sich dieses beim Gateway **200** an. Mit dieser Anmeldenachricht **12** (**Fig.** 3) überträgt das Gerät **100** seine GUID und vorteilhafter Weise auch seine Model ID. Außerdem beinhaltet die Nachricht auch eine Primzahl n, für die gilt: $(n-1)/2$ ist ebenfalls eine Primzahl und eine Primzahl g. Außerdem wählt das Gerät intern eine Zufallszahl x. Zusätzlich zu n und g wird noch das Ergebnis der Operation (g^x mod n) an das Gateway **200** übertragen. Das Gateway übernimmt alle diese Parameter und sendet sie an den internen Busmanager **300** weiter (**13**). Der Busmanager **300** wählt nun seinerseits eine Zufallszahl y und berechnet auf Basis der vom Gerät **100** übertragenen Werte das Ergebnis der Operation (g^y mod n). Dieses Ergebnis wird an das Gateway (**14**) und von dort an das Gerät **100** übermittelt (**15**). Mit Hilfe der Ergebnisse der beiden Operationen können nun sowohl das externe Gerät **100** und der Busmanager **300** das Ergebnis der Operation $K_{BB} = (g^{xy} \bmod n)$ berechnen. Dieses Ergebnis K_{EB} dient in der Folge als gemeinsamer Schlüssel (**16**) für die folgende Authentisierung. Diese Möglichkeit, einen gemeinsamen Schlüssel zu bestimmen, ohne dass ein Dritter diesen ermitteln kann, wird als Diffie-Hellmann Key-Exchange bezeichnet.

[0037] Nachdem ein gemeinsamer Schlüssel (**16**) sowohl im externen Gerät **100** als auch im Busmanager **300** existiert, wird die Authentisierung nach dem Challenge-Response Verfahren durchgeführt. Dabei generiert der Busmanager **300** eine Zufallszahl R_B (die sogenannte Challenge) und sendet (**17**, **18**) diese an das externe Gerät **100**. Das externe Gerät **100** verschlüsselt die Challenge mit dem gemeinsamen Schlüssel K_{EB} und sendet das Ergebnis (**19**) über das Gateway **200** zurück (**20**) an den Busmanager (sogenannter Response). Außerdem enthält diese Nachricht eine Zufallszahl R_E, die als Challenge dem Busmanager gesendet wird. Der überprüft jetzt, ob die Zufallszahl R_B mit dem korrekten Schlüssel K_{EB} verschlüsselt wurde. Nach der

Verifikation verschlüsselt der Busmanager die Challenge R_E ebenfalls mit dem Schlüssel K_{EB} und sendet das Ergebnis (21, 22) an das externe Gerät 100. Dieses überprüft seinerseits die Richtigkeit des Ergebnisses. Wenn beide Überprüfungen ein korrektes Ergebnis geliefert haben, haben sich beide Kommunikationspartner (Gerät 100 und Busmanager 300) authentifiziert. Der Busmanager kann jetzt aufgrund der in der GUID enthaltenen Herstellerkennung, anhand der in der GUID enthaltenen Seriennummer oder besonders vorteilhaft der Model ID den Zugriff auf bestimmte Ressourcen des Netzes erlauben oder auch sperren.

[0038] Besonders vorteilhaft beinhaltet ein Gateway 200 neben der Umsetzung von physikalischen Gegebenheiten und/oder Protokollen auch eine Firewallfunktionalität 201. Dabei wird in besonders vorteilhafter Weise das zuvor beschriebene Verfahren zur Authentisierung genutzt, um festzustellen, welche Ressourcen ein externes Gerät auf welche Art und Weise verwenden und/oder kontrollieren darf.

[0039] Der Busmanager 300 erkennt aufgrund der in der GUID enthaltenen Herstellerkennung (Vendor ID) und/oder der Seriennummer und/oder der zusätzlichen Model ID um welchen Gerätetyp, beziehungsweise auch um welches Gerät es sich bei dem externen Gerät handelt. Nach einem internen Verfahren legt der Busmanager 300 die Zugriffsberechtigungen auf die Netzelemente für dieses Gerät 100 fest. Aufgrund dieser ermittelten Zugriffsberechtigungen konfiguriert (24) der Busmanager 300 das Firewall-Modul 201 innerhalb des Gateways 200 so, dass dieses entsprechend der festgelegten Berechtigungen sperrt oder öffnet. Dabei können die Berechtigungen aufgrund der Quelladresse, d. h. der Herkunftsadresse eines Datenpaketes oder aufgrund der Zieladresse eines Datenpaketes eingestellt werden. Möglich, aber aufwendiger ist eine Filterung bestimmter Kommandos. Dabei muss die Firewall ein Datenpaket jedoch sehr detailliert auswerten.

[0040] Im Ausführungsbeispiel gemäss **Fig.** 2 ist ein externes Gerät 100 über eine Funkschnittstelle an ein Gateway 200 mit dem fahrzeuginternen Netzwerk 1 verbunden. Im fahrzeuginternen Netzwerk befindet sich mindestens ein als Busmanager (Busmaster) ausgezeichnetes Gerät 300 und ein weiteres Gerät 400.

[0041] In diesem Beispiel wird angenommen, dass es sich bei dem externen Gerät um ein Werkstattdiagnosegerät handelt. Dieses Diagnosegerät beinhaltet eine Funktion, mit der es möglich ist, eine Kommunikation auf dem fahrzeuginternen Gerät 400 durchzuführen und auf diesem Gerät, z. B. eine zentrale Steuereinheit, Einstellung auszulesen und zu verändern. Da diese Veränderungen bei einer fehlerhaften Bedienung Einfluß auf die Funktion des Gerätes oder des Fahrzeuges haben können, ist für den Zugriff auf diese Steuereinheit eine Authentifizierung vorgesehen, d. h. das Diagnosegerät erhält nur Zugriff auf die Steuereinheit, wenn sich das Gerät und/oder der Anwender gegenüber dem Busmanager 300 authentifiziert. Dazu tauschen das Diagnosegerät und der Busmanager zunächst einen Schlüsselsatz aus, um die nachfolgende Authentifizierung durchführen zu können. Anschließend wird eine Authentifizierung durchgeführt. Nach der erfolgreichen Authentifizierung entscheidet der Busmanager, welche Art von Zugriff das Diagnosegerät auf die Elemente des fahrzeuginternen Netzwerkes erhält und konfiguriert das Firewall-Modul 201 innerhalb des Gateways 200 entsprechend. In diesem Beispiel erkennt der Busmanager ein autorisiertes Diagnosegerät des Fahrzeugherstellers und gibt vollen Zugriff auf alle Geräte des Netzwerkes frei. Damit kann jetzt beispielsweise eine Aktualisierung von Betriebs- oder Anwendungssoftware oder eine Fehlerdiagnose des Systems durchgeführt werden.

[0042] In einem weiteren Ausführungsbeispiel nach **Fig.** 1 ist das extern angeschlossene Gerät diesmal kein autorisiertes Diagnosegerät, sondern ein Handheld-Computer, mit dem ein Anwender Informationen zu einem im Fahrzeug installierten Gerät, z. B. Navigationsgerät 400, übertragen möchte. Nach der Authentifizierungsprozedur schaltet der Busmanager 300 im Firewall-Modul 201 für das externe Gerät 100 nur den Zugriff auf das Navigationsgerät 400 mit den für den Datenaustausch benötigten Steuerbefehlen frei. Ein Zugriff auf andere Geräte oder anderen Befehlen ist im externen Gerät nicht möglich, da diese vom Firewall-Modul blockiert werden.

[0043] Alternativ können die Zugangsberechtigungen zwischen dem Busmanager 300 und dem externen Gerät 100 verhandelt werden. Dabei kann das externe Gerät bestimmte Zugriffsberechtigungen anfordern, die der Busmanager dann gewähren oder ablehnen kann.

[0044] Anstelle eines an das Gateway 200 angeschlossenen externen Gerätes 100 kann auch ein externes Netzwerk angeschlossen werden, das mit dem Netzwerk in Kommunikationsverbindung treten möchte. Die Prozeduren der Identifikation und der Authentifizierung laufen wie zuvor geschildert ab. Das Netzwerk kann natürlich auch mehrere Gateways aufweisen, über die mehrere Geräte oder Netze angeschlossen sind, die zeitlich gestaffelt oder gleichzeitig auf das Bussystem oder Netz zugreifen. Insbesondere bei einem gleichzeitigen Zugriffswunsch auf die gleiche Ressource, gewährt der Busmanager 300 den Zugriff nach zuvor vereinbarten Prioritäten oder durch Verhandlung.

Literatur

[1] IEEE, "P1394a Draft for a High Performance Serial Bus (Supplement)",

[2] HAVi Organization, "The HAVi Specification 1.0",

[3] Andrew S. Tanenbaum, "Computernetzwerke", Prentice Hall, 1998

Patentansprüche

1. Verfahren zur Steuerung des Zugriffs auf Elemente innerhalb eines Bussystems oder Netzes mit folgenden Schritten:
   - ein externes Gerät (100), das mit dem Bussystem oder Netz in Kommunikationsverbindung treten möchte, identifiziert sich über eine gerätespezifische Kennung bei einem Bus- oder Netzmanager (300), wobei die gerätespezifische Kennung selbst oder ein ihr zugeordneter Datensatz Angaben über die Zugehörigkeit des Gerätes zu einer bestimmten Klasse enthält,
   - es wird eine Authentifizierung des externen Gerätes (100) anhand eines digitalen Schlüssels vorgenommen,
   - nach der Authentifizierung wird dem externen Gerät (100) ein Zugriff entsprechend seiner Klassenzugehörigkeit auf Elemente des Bussystems oder Netzes gewährt.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass sich das externe Gerät (100) für den Zugriff bei einem Gateway (200) mittels einer Anmeldenachricht anmeldet, welche insbesondere zusammen mit der Gerätekennung zum Bus- oder Netzmanager (300) übertragen wird.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass neben der gerätespezifischen Kennung auch eine Geräteklassenkennung übertragen wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass eine gemeinsame Schlüs-

selvereinbarung zwischen dem externen Gerät (**100**) und dem Bus- oder Netzmanager (**300**) vorgenommen wird, insbesondere durch den Austausch von Parametern, wie Primzahlen, Zufallszahlen und deren Verknüpfungen.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass zur gemeinsamen Schlüsselvereinbarung das Diffie-Hellmann Verfahren verwendet wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass nach der gemeinsamen Schlüsselvereinbarung zwischen dem externen Gerät (**100**) und dem Bus- oder Netzmanager (**300**) eine Authentisierung nach dem Challenge-Response Verfahren durchgeführt wird.

7. Verfahren nach einem der Ansprüche 2 bis 6, dadurch gekennzeichnet, dass das Gateway (**100**) eingerichtet ist, Signalumsetzungen nach dem ISO/OSI-Schichtenmodell zumindest in der Physical-Layer und/oder höherer Schichten durchzuführen.

8. Verfahren nach einem der Ansprüche 2 bis 7, dadurch gekennzeichnet, dass das Gateway (**200**) eingerichtet ist, eine Firewallfunktionalität (**201**) durchzuführen.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass die Authentisierung dazu genutzt wird, festzustellen, welche Ressourcen des Bussystems oder Netzes das externe Gerät (**100**) auf welche Art und Weise verwenden und/oder kontrollieren darf.

10. Verfahren nach einem der Ansprüche 8 oder 9, dadurch gekennzeichnet, dass der Bus- oder Netzmanager (**300**) aufgrund der von ihm ermittelten Zugriffsberechtigung die Firewallfunktionalität (**201**) so konfiguriert, dass diese entsprechend der ermittelten Zugriffsberechtigung, eine Freigabe oder Sperrung der Ressourcen des Bussystems oder Netzes vornimmt.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Freigabe oder Sperrung aufgrund der Quelladresse oder der Zieladresse eines Datenpaketes vorgenommen wird.

12. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Firewallfunktionalität (**201**) entsprechend der ermittelten Zugriffsberechtigung, bestimmte Kommandos des externen Gerätes (**100**) filtert.

13. Verfahren nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass die Zugriffsberechtigung zwischen dem externen Gerät (**100**) und dem Bus- oder Netzmanager (**300**) ausgehandelt wird.

14. Verfahren nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, dass anstelle eines externen Gerätes (**100**) oder zusätzlich ein externes Bussystem oder Netz eine Kommunikationsverbindung mit dem Bussystem oder Netz aufnimmt, um einen Zugriff auf Elemente des Bussystems oder Netzes zu erhalten.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 45 975 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 11. April 2002

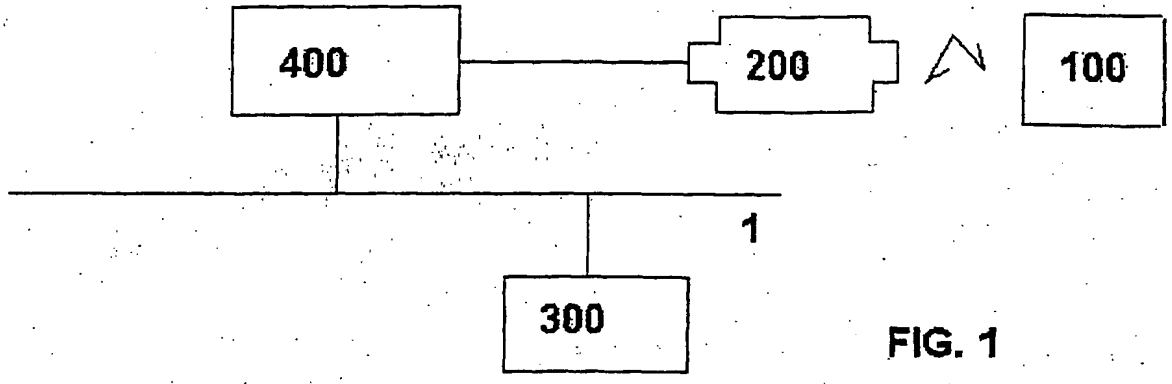


FIG. 1

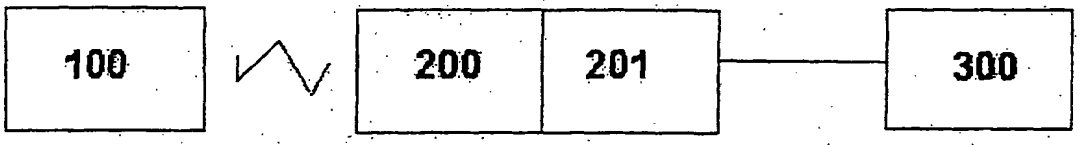


FIG. 2

Nummer: DE 100 45 975 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 11. April 2002

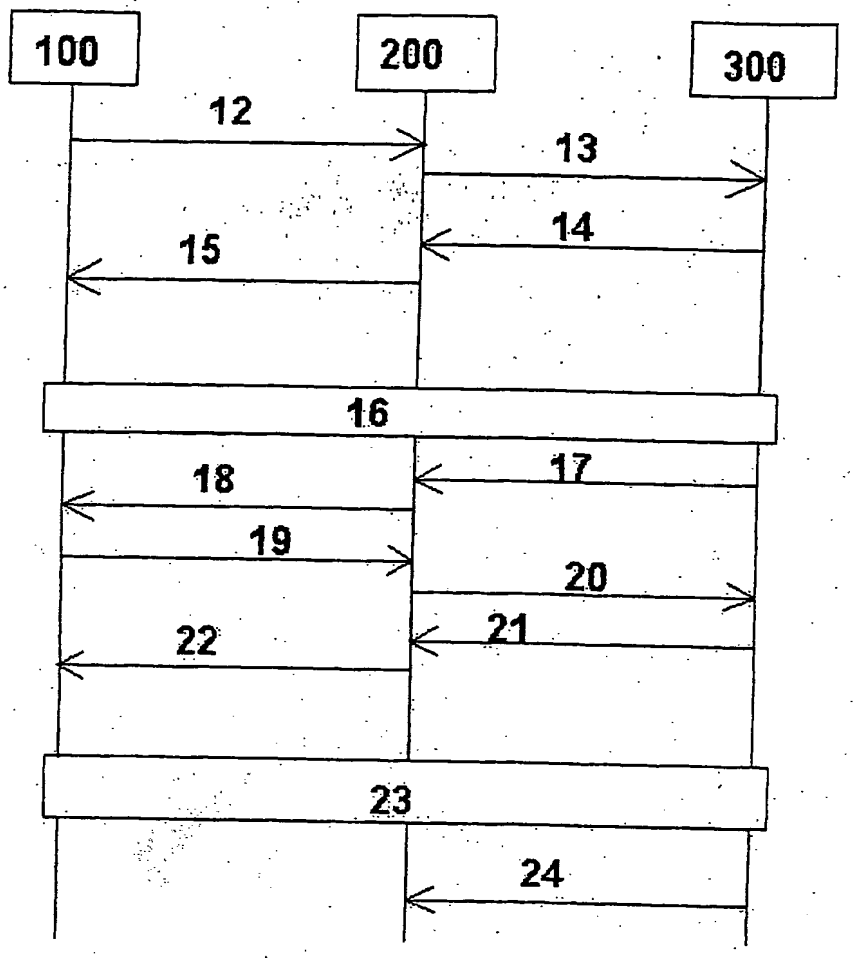


FIG. 3